Projet

INCOGNITO

Comment concilier informatique et mécanique pour faire une machine de chiffrement moderne inspirée d'Enigma ?

Note : Des liens hypertexte sont présents dans le Powerpoint, afin de compléter les informations si vous voulez des détails.

AUDRAS Pauline
MEIER Louise
MICHELETTI Nicolas
MOREAU Rémi

Sommaire

Introduction : Résumé du projet et membres de l'équipe

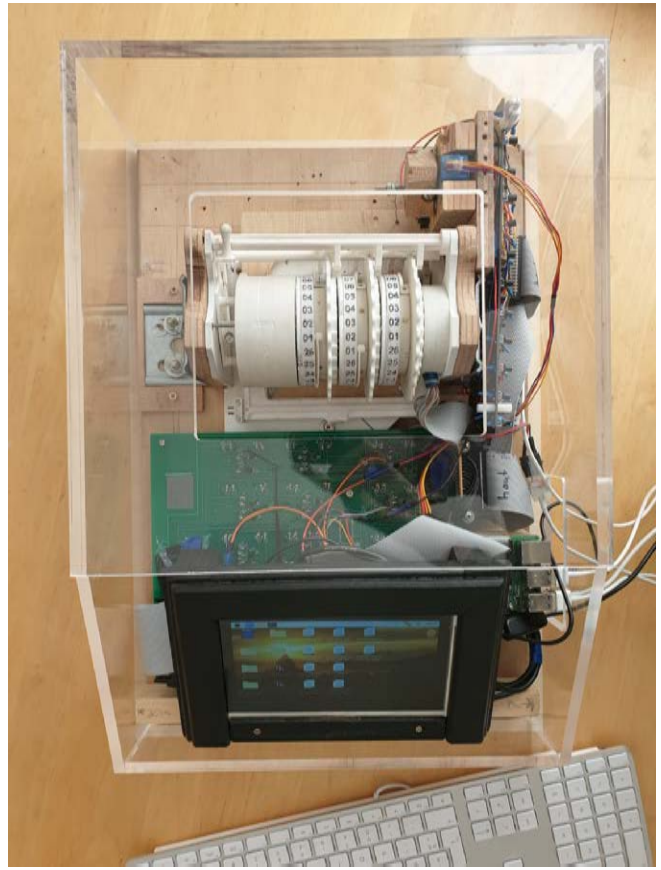
I. Enigma : Histoire et fonctionnement
II. D' Enigma à InCOGnito
III. Conception théorique
IV. Fabrication
V. Que pouvons-nous améliorer?

Conclusion

Remerciements

Résumé du projet InCOGnito

- Le **projet InCOGnito** est né de la volonté de 4 élèves de s'ouvrir sur le monde des sciences de l'ingénieur et la gestion de projet.
- L'idée germe au mois d'**août 2020**, d'après le constat suivant : si un chiffrement est fait sur un ordinateur, rien ne protège le message chiffré dans un ordinateur piraté ; seul un chiffrage mécanique assurerait son inviolabilité. Nous avons décidé de nous inspirer de la machine de chiffrement **ENIGMA** pour l'adapter et l'intégrer à un environnement de bureautique moderne dans l'optique d'allier l'ergonomie de la technologie et le chiffrement mécanique.
- Le défi du projet consiste donc à maîtriser à la fois **l'aspect mécanique** de la machine ENIGMA, mais également faire communiquer cette partie mécanique avec un **clavier informatique** et un **ordinateur**.
- Pour parvenir à nos fins, nous dûmes élargir nos connaissances dans de nombreux domaines, notamment **l'informatique**, **l'électronique**, la **mécanique**. Notre objectif, découvrir les sciences de l'ingénieur, fut atteint !



ND: le chiffrement est un procédé en cryptographie dont le but est de rendre incompréhensible le message à toute personne n'ayant pas la clé de déchiffrement

Membres de l’équipe

Pauline Audras

Elève de Terminale
Spécialités Mathématiques-Physique

Projet d’étude: Ingénierie ou recherche en physique
Hobby: Art, sciences et littérature

Responsable du domaine mécanique :
Impression et montage des pièces 3D et application du moteur

Louise Meier

Elève de Terminale
Spécialités Mathématiques-Physique

Projet d’étude: Ingénierie ou recherche en physique
Hobby: Littérature, sciences physique et mathématiques

Responsable du domaine mécanique :
Impression et montage des pièces 3D et application du moteur
Responsable du contact avec le Professeur Simon Wiest ainsi qu’avec M. Ertel

Nicolas Micheletti

Elève de Terminale
Spécialités Mathématiques-Physique

Projet d’étude: ingénieur via CPGE / UTC
Hobby: musique (pratique du piano et de la batterie), escrime, jeux-vidéos, physique

Responsable du domaine électronique *:*
Création du circuit imprimé et application du moteur

Rémi Moreau

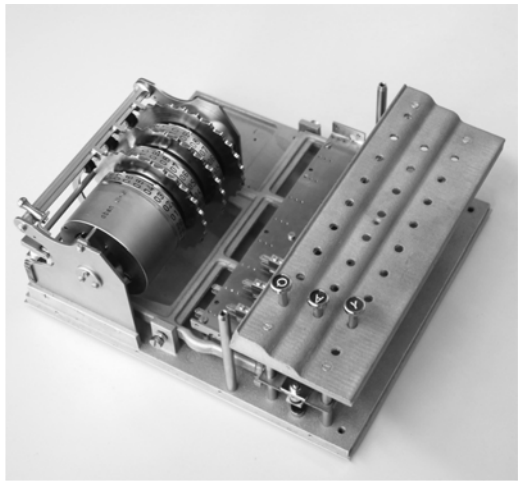
Elève de Terminale
Spécialités Mathématiques-Physique

Projet d’étude: ingénieur en spatial (fuséologie) via CPGE
Hobby: lecture (classique, historique, scientifique, actualité), escalade, jeux-vidéos

Responsable du domaine informatique :
Codage de la Raspberry Pi et application du moteur

Enigma et ses descendants…

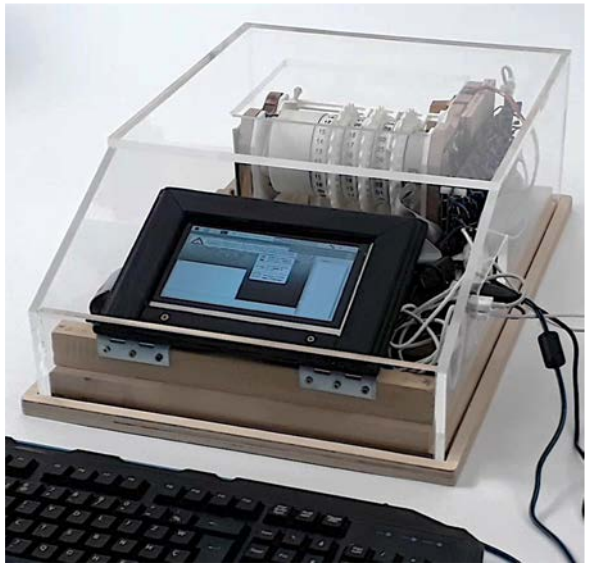
Enigma 1930



Weingarten 2011
Hochschule Ravensburg-Weingarten
Réalisation à l'identique

Enigma RDE 2020
Hochschule der Medien Stuttgart
Réalisation en impression 3D

Notre réalisation



InCOGnito 2021
Institut Montalembert, Nogent sur Marne
Réalisation hybride

Enigma : Histoire

La machine Enigma fut parmi les plus grandes avancées en cryptographie

- 1918 : Création par Scherbius et première vraie mécanisation du chiffrage
- 1928 : Début de l'utilisation d'Enigma par tous les corps de l'armée allemande

- 1932 : Les Polonais cassent le chiffre d'Enigma
- 1938 : Les Allemands deviennent plus prudents sur l'utilisation du chiffre et modifient la machine. Les travaux des Polonais deviennent laborieux.
- 1939 : Invasion de la Pologne. Les travaux polonais sont envoyés aux Anglais et aux Français qui jusqu'alors n'avaient aucune idée de comment contrer Enigma
- 1942 : Turing casse le chiffre d'Enigma définitivement à l'aide des « bombes de Turing » (précurseur de l'ordinateur) sans que l'armée allemande s'en rende compte. Cela aurait d'après certaines estimations permis de raccourcir la guerre de 2 ans.

Enigma : Fonctionnement

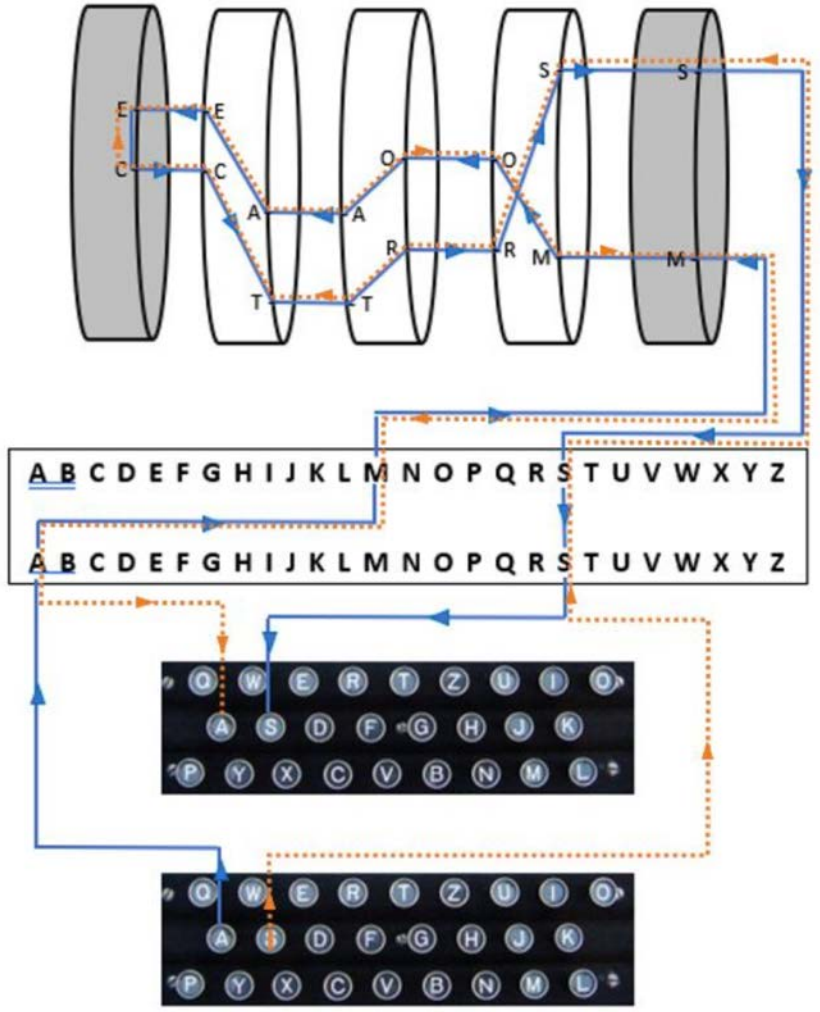
1. Composition de la machine

1. **Clavier** : transmet le mouvement mécanique (appui de la touche quand message tapé) en signal électrique
2. **Tableau de connexions** : inter-change les lettres de façon fixe
3. **Rotors (ou brouilleurs) :** tournent de façon désolidarisée. Indépendamment, ont des réglages définis (par exemple A devient B dans le rotor III).
4. **Rotor de retour (ou réflecteur) :** permet de faire retourner le signal dans les rotors
5. **Tableau de lampes :** Visualisation du message modifié (chiffré ou déchiffré)

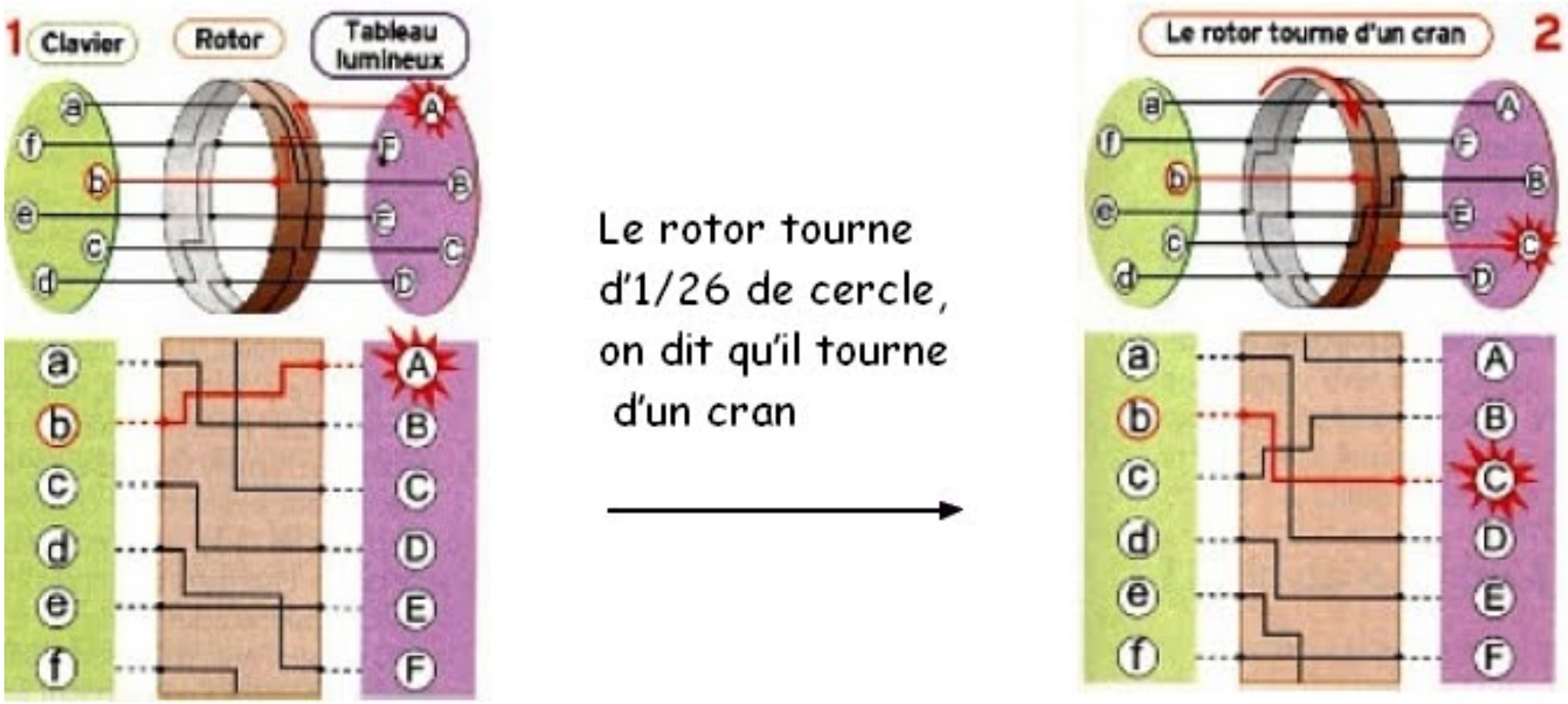
Enigma : Fonctionnement

2. Principe de fonctionnement

- Appui sur une touche du clavier
- Déclenchement du signal électrique correspondant et rotation du premier rotor.
- Passage dans le tableau de connexions : la lettre change potentiellement selon les réglages.
- Entrée du signal dans les rotors
- Transformation de la lettre dans les rotors
- Retour du signal : 2^{e} passage dans le tableau de connexions
- Récupération du signal chiffré grâce au tableau de lampes



Au bout de 26 rotations du 1er rotor (alphabet complet), le 2ème rotor tourne d'un cran.
Au bout de 26 rotations du 2ème rotor (donc 26x26 rotations du 1er), le 3ème rotor tourne d'un cran.
La position initiale est donc retrouvée au bout de 17 576 rotations du 1er rotor (une fois que le 3ème a fait 26 rotations).



Les 3 rouleaux sont interchangeables (la plupart des modèles Enigma avaient 5 rotors à disposition).
La rotation des rotors permet d'empêcher l'analyse de fréquence.

D’ Enigma à InCOGnito

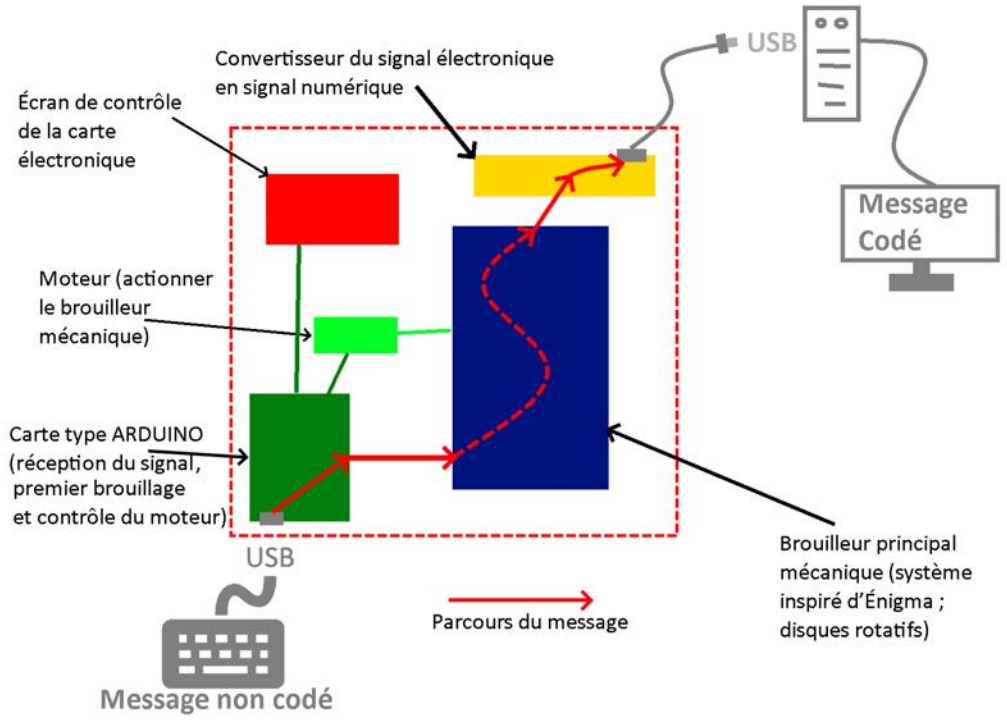
1. Innovations

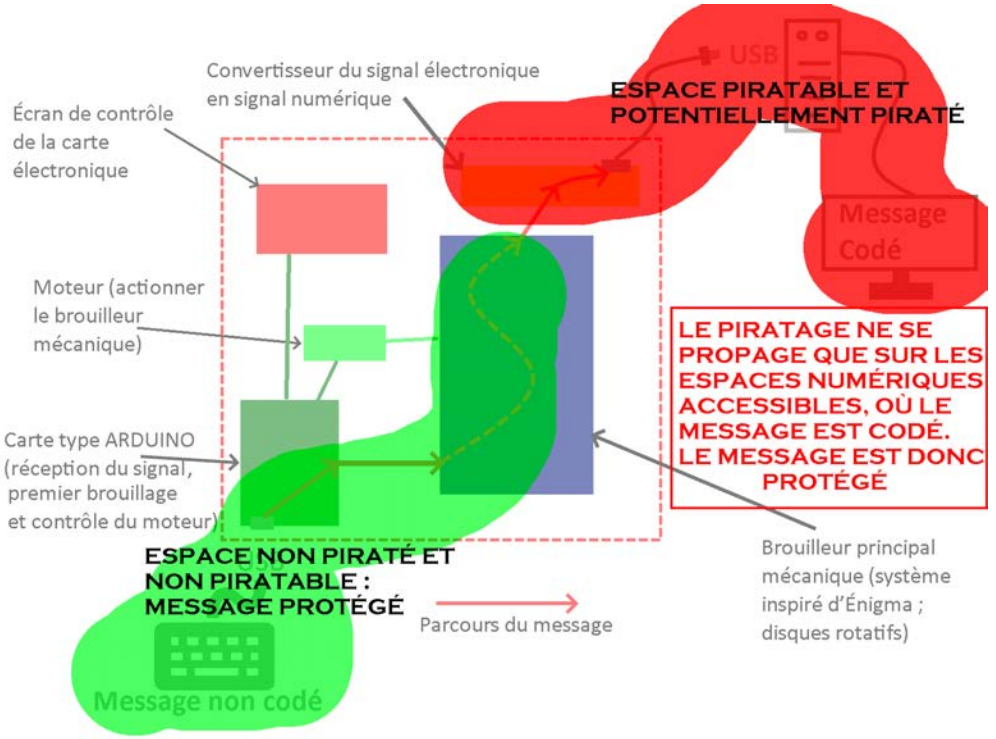
- **InCOGnito** conserve le même fonctionnement mécanique qu’Enigma au niveau des rotors (mais ceux-ci sont fabriqués en impression 3D).

- **InCOGnito** s’intègre au domaine numérique, informatique et électronique :

  - message tapé sur un clavier branché par USB
  - tableau de connexions géré par un microordinateur (RaspberryPi)
  - écran commandé par la RaspberryPi, comme interface avec l’utilisateur
  - message chiffré reçu par l’ordinateur par câble USB
  - utilisation d’un moteur afin de faire tourner les rotors

- **InCOGnito** prévient et rend impossible l'accès au message clair en cas de piratage de l'ordinateur grâce à son intermédiaire mécanique





- **InCOGnito** innove par « l'invention » d'un modèle asymétrique, qui corrige une erreur majeure d'Enigma :

Une grande faiblesse d'**Enigma** est qu'une lettre ne peut être chiffrée en elle-même (X ne peut pas être chiffré en X) à cause d'un double passage dans le tableau de connexion à l'aller et au retour (sachant qu'une lettre ne peut devenir elle-même dans les rotors).

Cette faille est utilisée par la machine de Turing pour casser le chiffre d'Enigma.

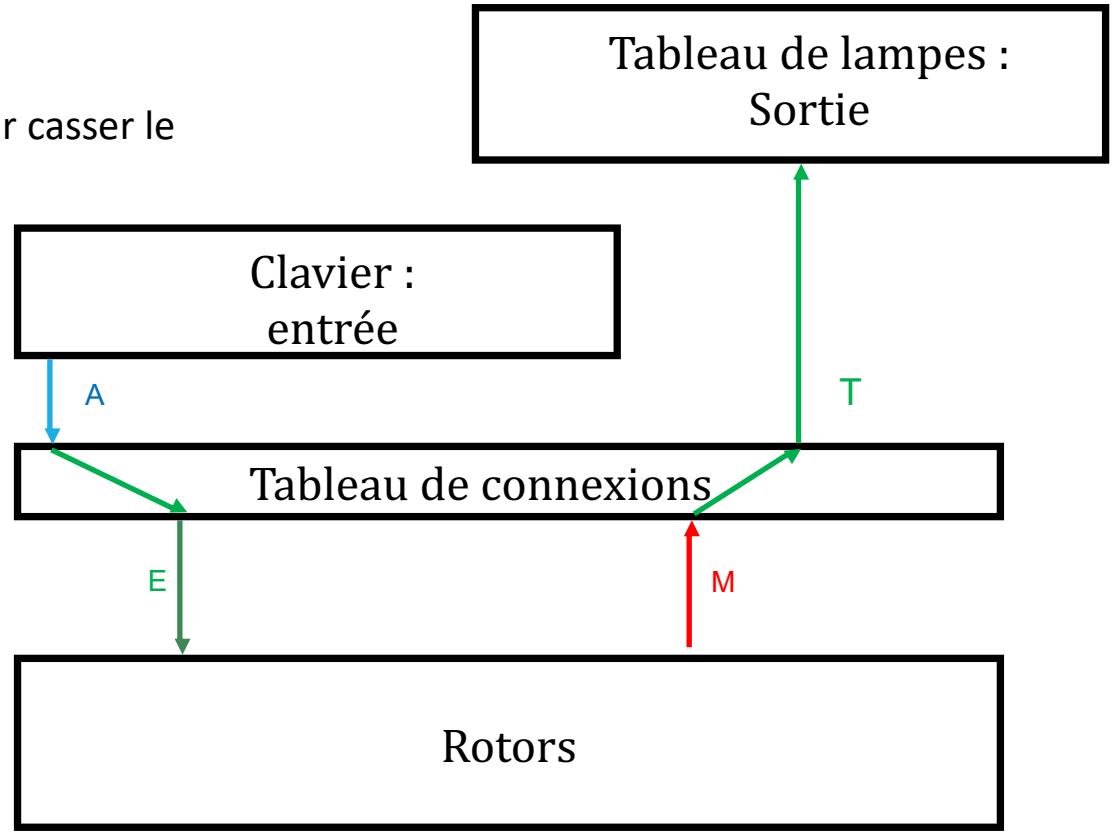


Schéma de représentation du modèle symétrique d'Enigma

Dans **InCOGnito**, il n'y a qu'un seul passage dans le tableau de connexion, ce qui impose un mode chiffrement et un mode déchiffrement. *Par exemple:*

Mode chiffrement : Entrée : A.

A -> E (tableau de connexions).

E -> M (rotors).

Sortie: M

Mode déchiffrement : Entrée : M

M -> E (rotors)

E -> A (tableau de connexions).

Sortie : A

Avec **InCOGnito**, le signal ne passe qu'une fois dans le tableau de connexions, cela permet donc qu'une lettre puisse être chiffrée en elle-même. *Par exemple :*

Entrée : X

X -> L (tableau de connexion)

L -> X (rotors)

Sortie : X

Pour déchiffrer il suffit de suivre le chemin inverse

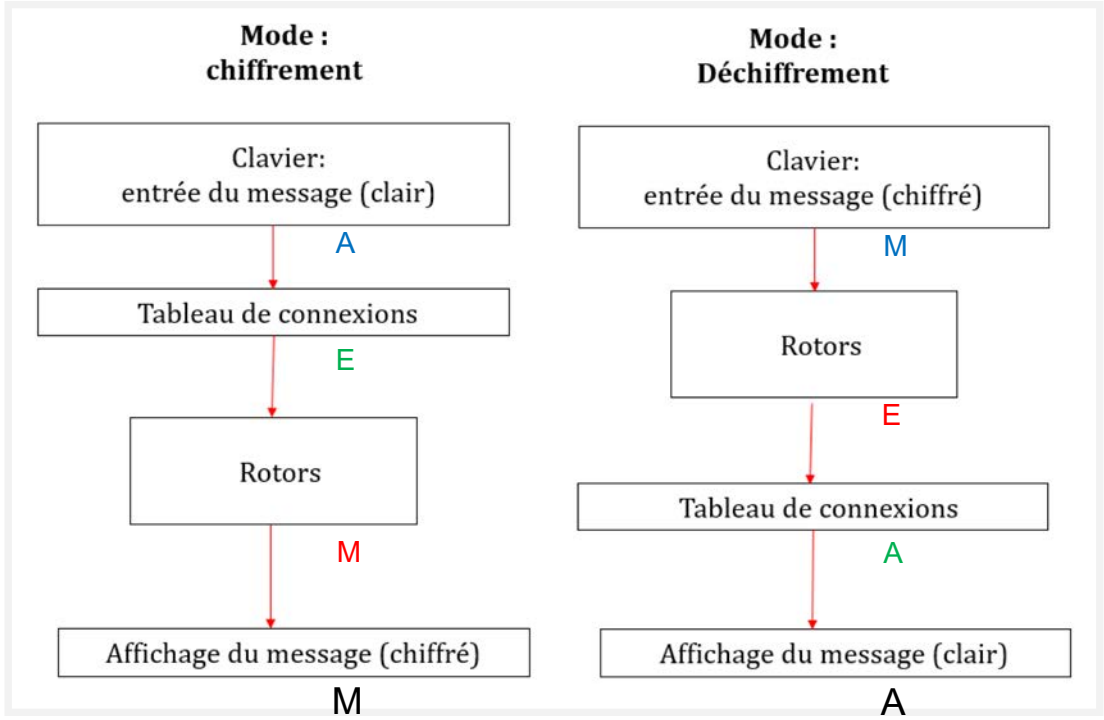


Schéma de représentation du modèle asymétrique

D' Enigma à InCOGnito

3. Efficacité du chiffre

- Dénombrement des possibilités d'**Enigma** :
  - Ordre des 3 rotors interchangeables (parmi les 5): 5!/2! = 5x4x3 = **60**
  - Position de départ des 3 rotors de 26 lettres: 26x26x26 = 26^3 = **17 576**
  - Tableau de connexions (les allemands utilisaient 6 câbles plutôt que 26) :

$$\frac{26\times25\times24\times23\times22\times21\times20\times19\times18\times17\times16\times15}{2^6\times6!} = 100\ 391\ 791\ 500 = \mathbf{1 \times 10^{11}}$$

Total : 60 x 17 576 x 100 391 791 500 = **$1{,}1 \times 10^{17}$**

- Dénombrement des possibilités d'**InCOGnito** :
  - Ordre des 3 rotors interchangeables : 3! = **6**
  - Position de départ des 3 rotors de 26 lettres : 26x26x26 = 26^3 = **17 576**
  - Tableau de connexions (chaque lettre peut devenir elle-même ou une autre) : 26! = **4×10^{26}**

Total : 6 x 17 576 x 4 x 10^{26} = **$4{,}3 \times 10^{31}$**

Soit 10^{14} fois plus efficace !

Conception théorique

1. Période : d'août à novembre 2020

Août à Octobre

Recherche de format de création des rotors :

- Possibilité d'utilisation d'une découpeuse laser (Fablab à proximité)
- Possibilité d'utilisation d'une imprimante 3D (Lycée Montalembert) qui sera le format utilisé

Septembre à Octobre

Découverte des projets allemands Weingarten et Enigma RDE :

- Contact en allemand avec M. Ertel du projet Weingarten
- Contact en allemand avec M. Wiest du projet Enigma RDE (entièrement mécanique et en impression 3D)

Novembre

Mise à disposition par M. Wiest des plans d'impression 3D.

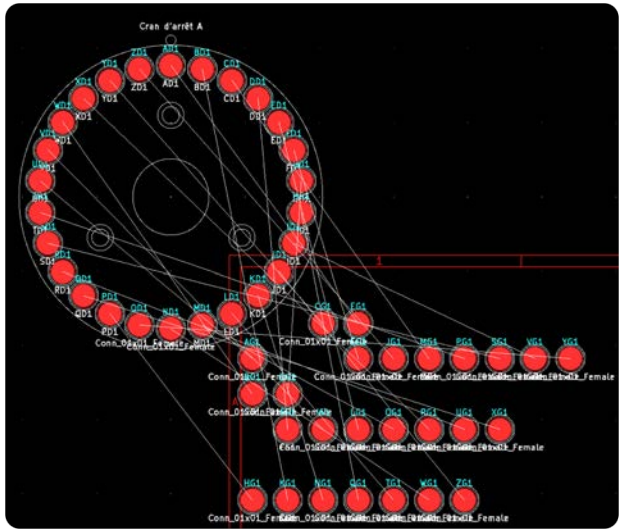
Professeur Simon Wiest et l'Enigma RDE

Conception théorique

2. Pistes de recherches

- Utilisation de circuits imprimés dessinés sur mesure dans les rotors (idée abandonnée)
  - **But** : éviter des branchements de câbles complexes
  - **Problème** : Principe de ressorts soudés est obsolète (distance trop grande) suite à l'observation des plans 3D du projet Enigma RDE

- Recherche du bon matériel pour les contacts sur les rotors.
  - **Besoin** : solidité (ne se raye pas), conduction électrique efficace, taille, forme (les contacts mâles retenus à l'intérieur des rotors à l'arrière)
  - **Idées** : fibre optique et lumière plutôt que des câbles conducteurs d'électricité, attaches parisiennes,…
  - **Solution:** rivets en cuivre (principe retrouvé dans Enigma RDE)



Essai de circuit imprimé

Rivets en cuivre utilisés

- Recherche d’un système mécanique pour gérer la rotation des rotors car InCOGnito ne dispose pas d’un clavier mécanique

  - utilisation d’un électroaimant

    Problème : manque de puissance, trop gourmand en énergie et non-linéaire

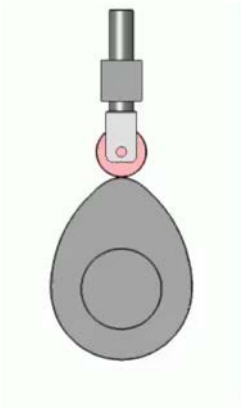
  - utilisation d’instruments optoélectroniques pour s’assurer du bon crantage lors du décalage (émetteur et détecteur de lumière)

    Problème : compliqué à mettre en place

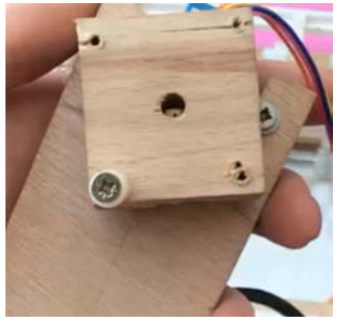
  - utilisation d’un ovale en bois relié à un moteur pas-à-pas pour faire monter et descendre un axe responsable de la rotation.

    Problème : Trop lent.

Solution : un carré qui tire une planche en bois, activant l’axe de bascule



Système avec l’ovale



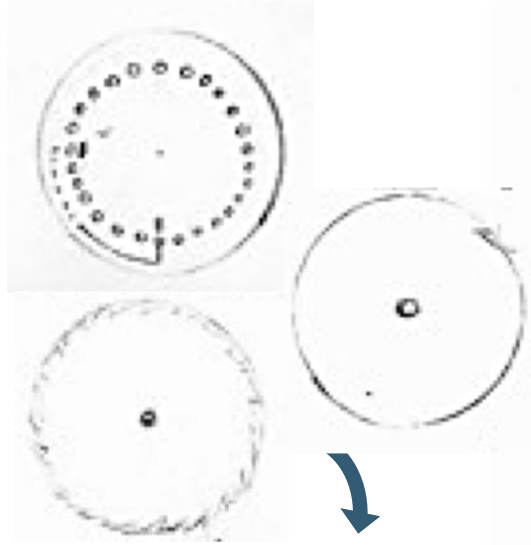
1er système du carré

2nd système du carré

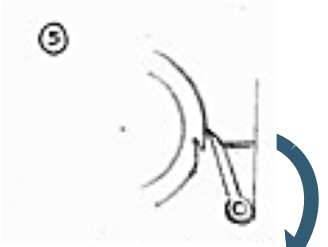
Bonus

Schéma de notre vision de la machine en septembre
(ne pas noter la piètre qualité des premiers schémas)

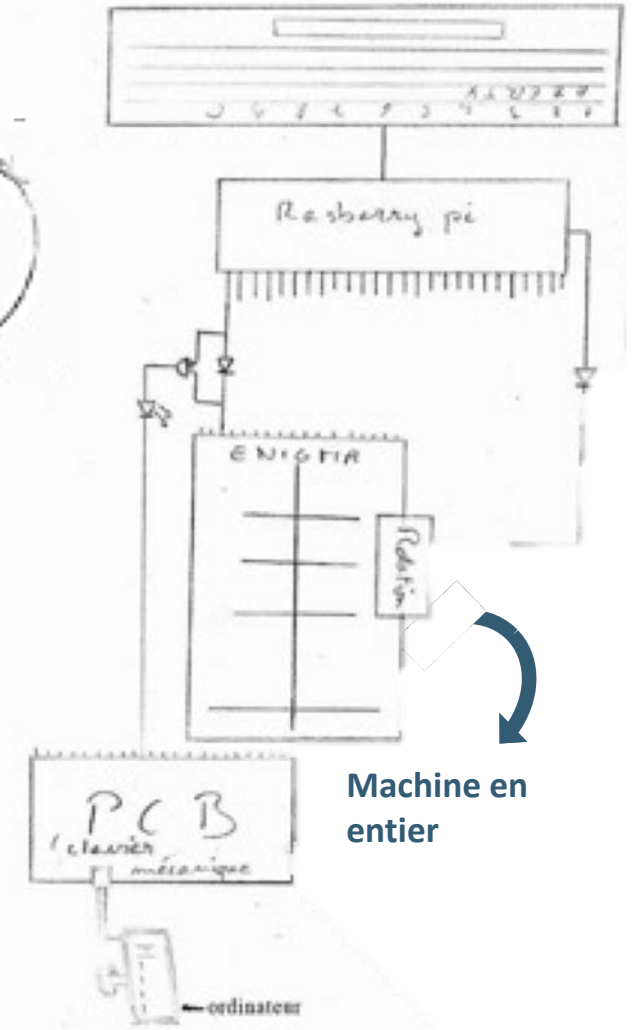
- Clavier : entrée des lettres
- RaspberryPi : tableau de connexions et 26 canaux de sortie
- Circuits intégrés avec 26 NOT et AND
- Rotors :
  - 3 rouleaux en rotation
  - 1 rouleau de retour
- Système de rotation :
  - 1 éléctroaimant sur un axe avec des dents de rotation
- PCB : 26 -> 1 canal (signal compréhensible par l'ordinateur)



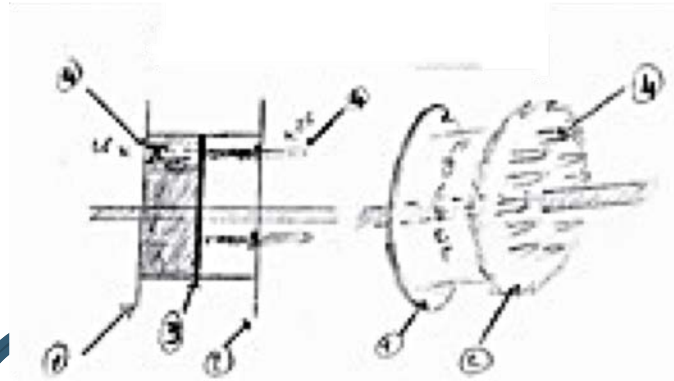
Rotors (interne, externe, dent de report)



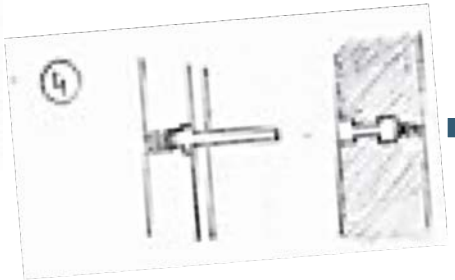
Dent de report



Machine en entier



Rouleau externe/interne



Connecteurs

Fabrication

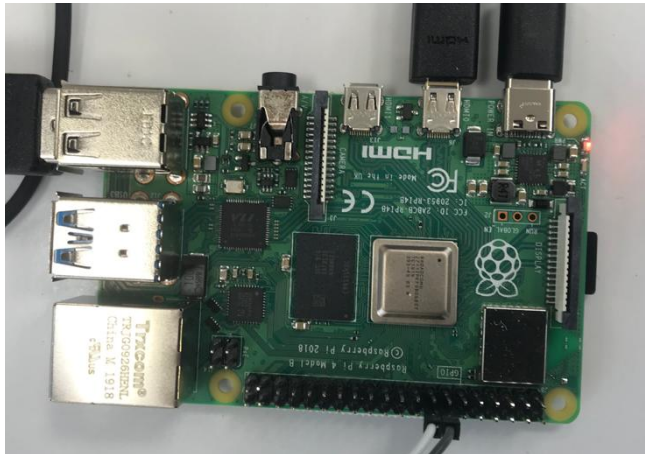
1. Numérique et informatique

Septembre à Novembre

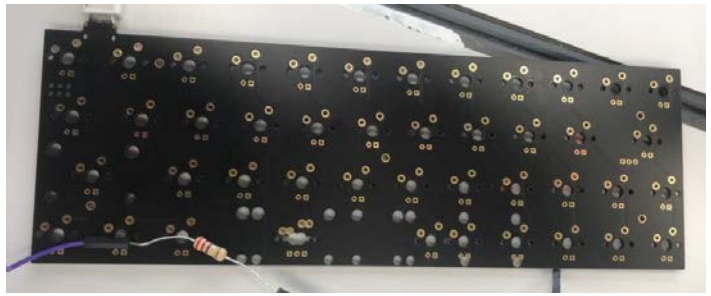
- Commande et réception de la RaspberryPi (1)
  RaspberryPi = nano ordinateur programmable de la taille d'une carte de crédit comprenant une connexion HDMI avec un écran

- Réception du clavier (2) qui transforme le signal électrique de sortie en lettre.

- Réception de l'écran (3)



1) RaspberryPi



2) Clavier

3) Ecran

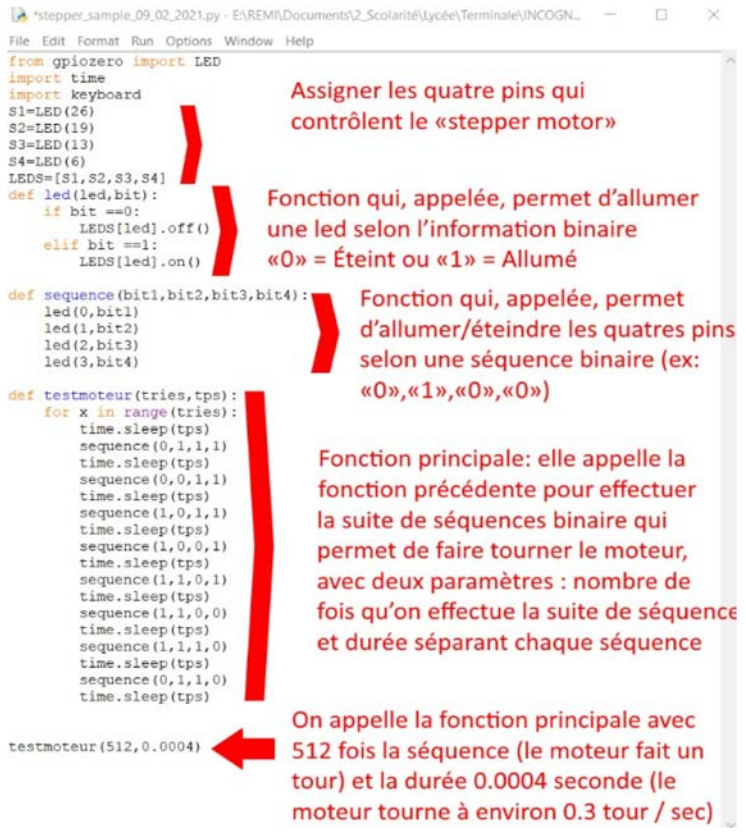
Fabrication

Octobre à Janvier

- Programmation du logiciel de la RaspberryPi avec une interface python (tkinter)

- Programmation de la clé de chiffrement en tableau de connexion valide, du chiffrage et déchiffrage du message

- Programmation du contrôle du moteur, du switch et des 26 lettres allant vers les rotors



Exemple d'algorithme pour faire fonctionner le moteur grâce à la RaspberryPi

Janvier à Mars

- Mise en place du switch (bouton pressoir, pour détecter quand les rotors ont avancé d'un cran) et du moteur (moteur pas-à-pas) reliés à la RaspberryPi

Problème : nombre de pins de la RaspberryPi insuffisant pour contrôler les 26 canaux (un par lettre), le moteur et le switch

Solution : utilisation d'un circuit d'extension MCP23017, contrôlé par l'interface I2C de la RaspberryPi

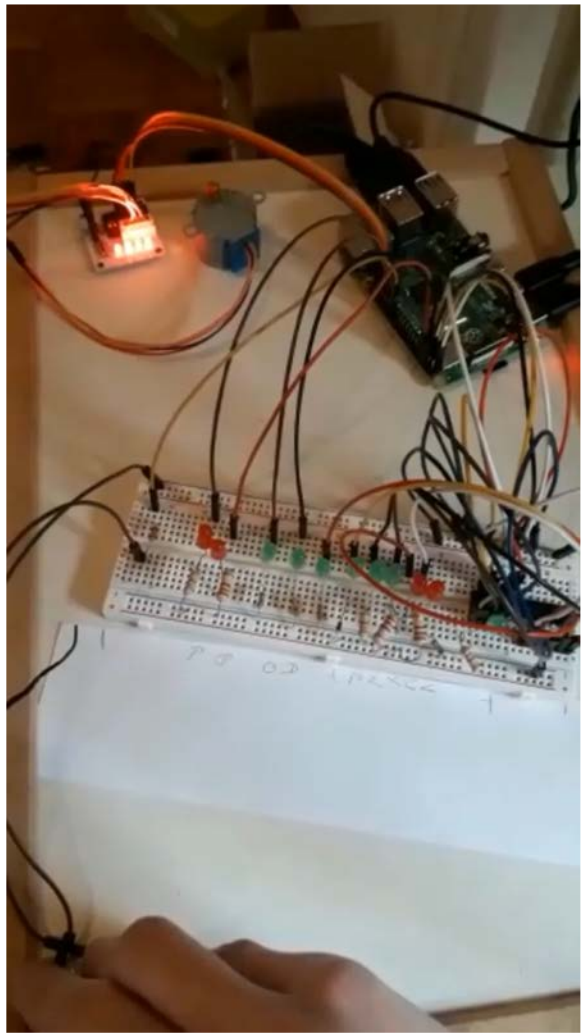
```
File  Edit  Format  Run  Options  Window  Help
from gpiozero import Button
from gpiozero import LED

led1=LED(26)
switch=Button(19)

while True:
    if switch.is_pressed():
        led1.on()
    else:
        led1.off()
```

Assigner les pins 26 et 19 à une led et à un switch

Si le switch est enfoncé, alors la led s'allume

La led s'éteint si le switch n'est plus enfoncé

Test d'allumage d'une LED avec bouton poussoir



Application du programme (LED, bouton poussoir et moteur)

Fabrication

2. Electronique

Août à septembre

- Définition du concept des interfaces possibles (micro-ordinateur, branchement clavier, sortie numérique, etc…)

Septembre à octobre

- Adaptation d’une carte pour clavier d’ordinateur pour sortir un signal numérique USB

Novembre à décembre

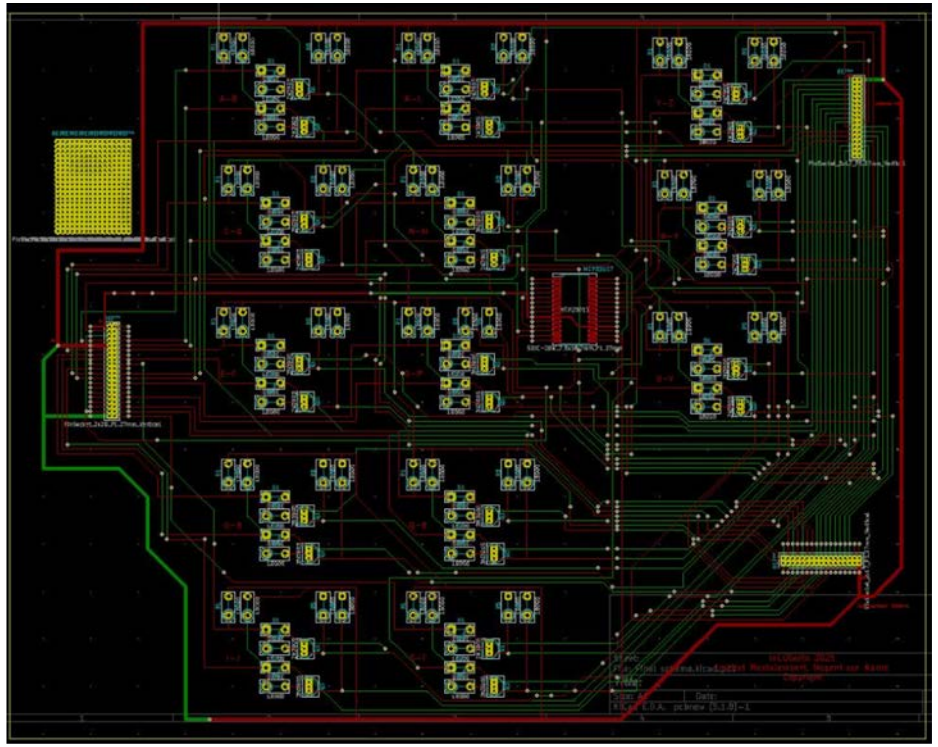
- Réflexion autour du circuit électrique (avec circuits intégrés et transistors)
- Idée d’utiliser des transistors sur la PCB clavier pour remplacer l’appui des touches manuelles

Novembre à Décembre

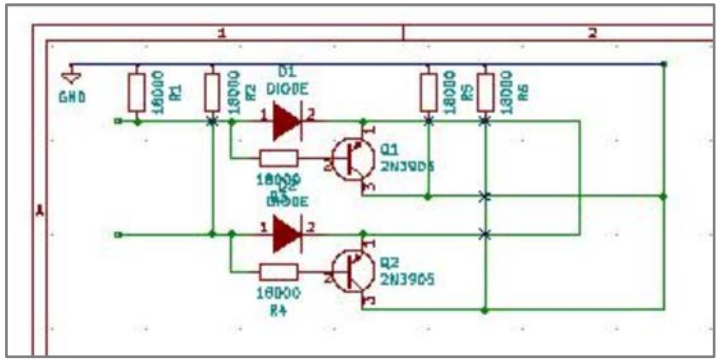
- Tests des transistors, de la RaspberryPi, transformation du signal numérique (clavier RaspberryPi) en signal électrique (Gpio RaspberryPi) puis à nouveau en sortie numérique avec une PCB « clavier » avec sortie USB

Janvier à Février

- Finalisation du circuit, tests en labo, apprentissage du logiciel KiCAD
- Design de la PCB
- Commande de la PCB



PCB (image KiCAD)



Détail du schéma électrique de la PCB (image KiCAD)

Fabrication

3. Mécanique

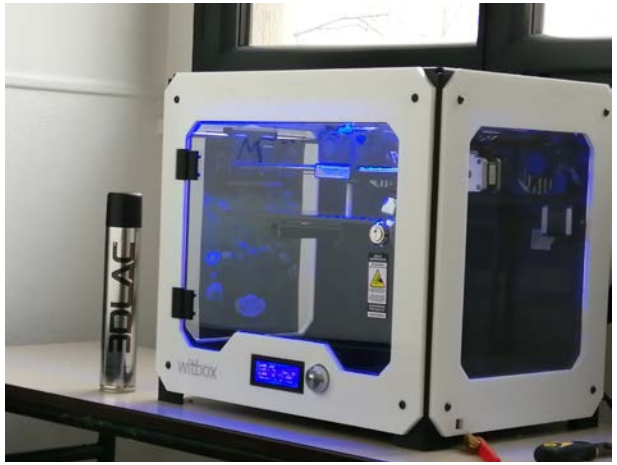
Novembre

- Obtention des fichiers 3D du projet Enigma RDE de la Hochschule der Medien de Stuttgart

Fichiers 3D

Décembre à Février

- Réparation et utilisation de l'imprimante 3D de l'Institut Montalembert
- Impressions tumultueuses des premières pièces : mauvaise qualité à cause des problèmes de l'imprimante



Imprimante 3D Witbox utilisée

Janvier

- Recherche de matériaux et pièces semblables à ceux conseillés par le projet Enigma RDE mais moins chers et livrant en France (ressorts, contacts, câbles électriques de 0,037mm^2…)

Février

- Découverte de différentes techniques (souder, scier, poncer…)
- Construction durant toutes les vacances (2 semaines) des rotors
- Montage de la machine et résolution du problème de couplage entre les rotors et le moteur et de la stabilité des pièces imprimées en 3D
- Impressions de dernière minute de pièces cassées grâce à l'imprimante de la médiathèque Louis Aragon de Fontenay-sous-Bois

Fabrication

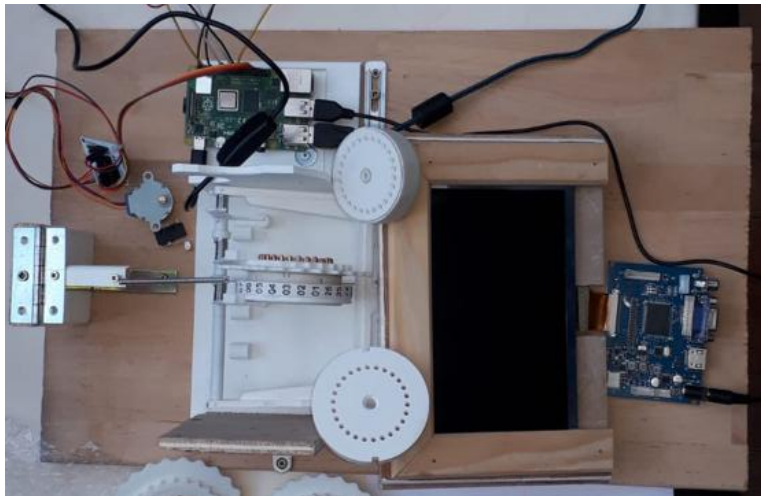
4. Boîte

Février

- Installation des pièces d'InCOGnito sur une planche de bois

Début mars

- Fabrication de la boîte en plexiglas protégeant la machine

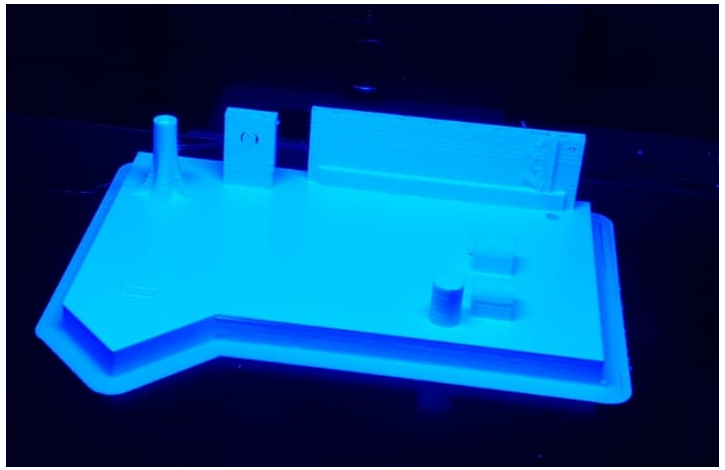


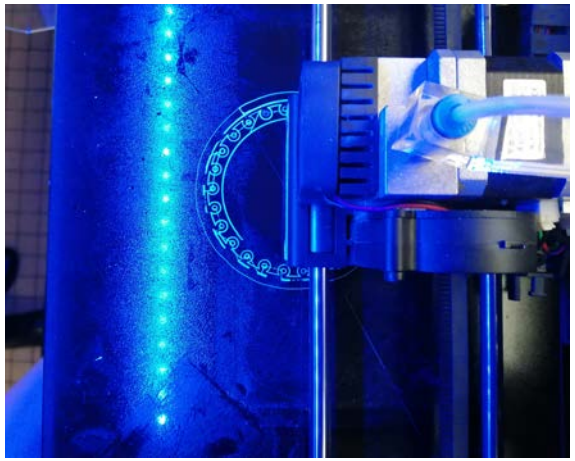
InCOGnito au début

InCOGnito avec la boîte en plexiglas

Bonus

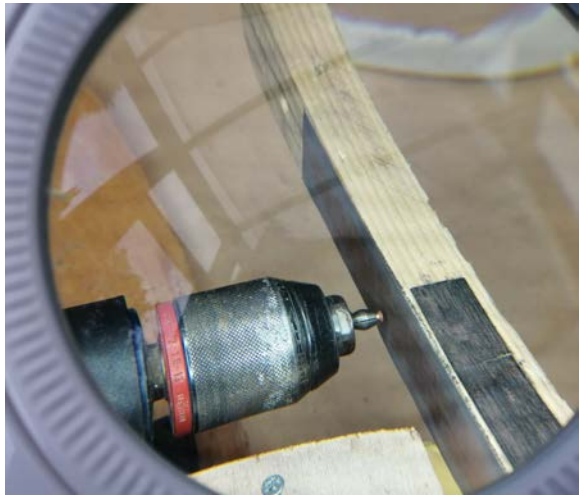
Problèmes d'imprimante 3D…

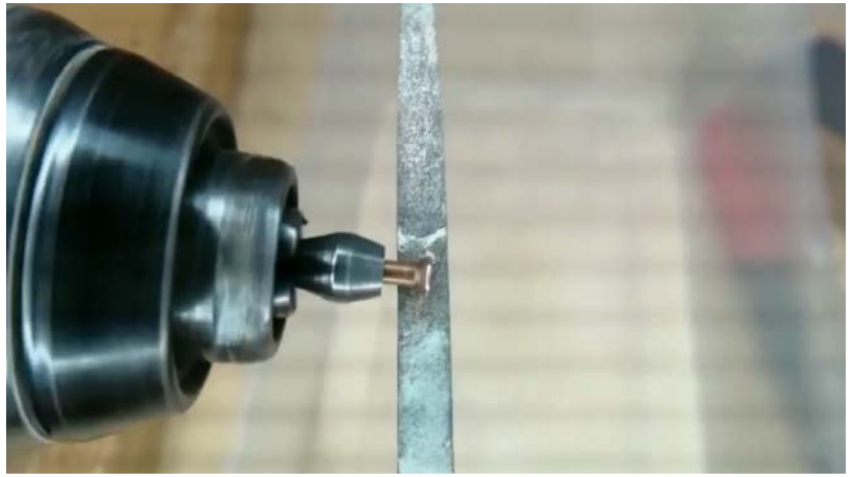




Bonus

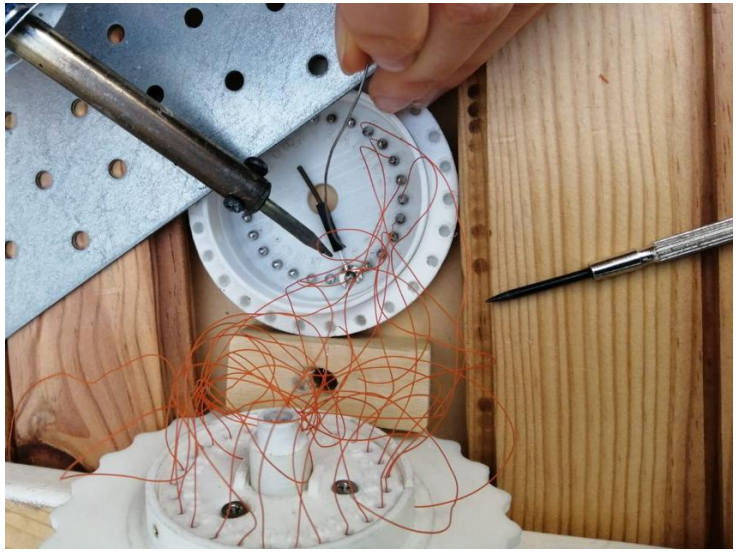
… étape de ponçage…

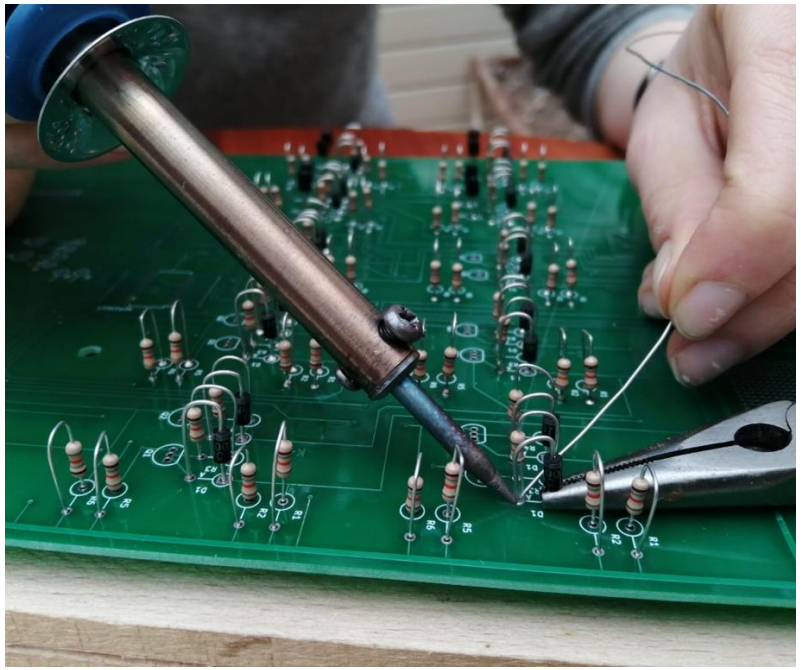


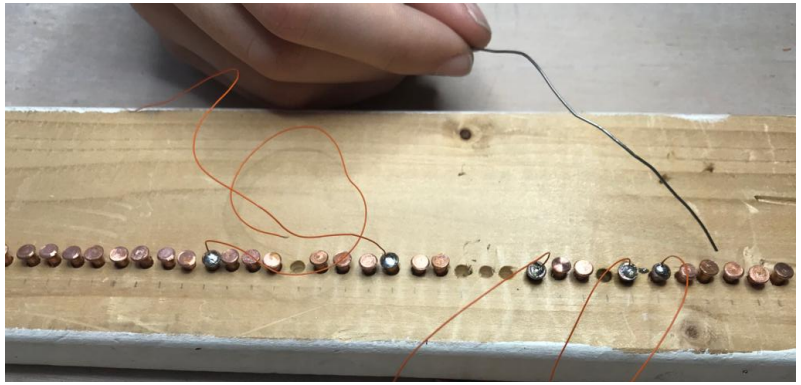


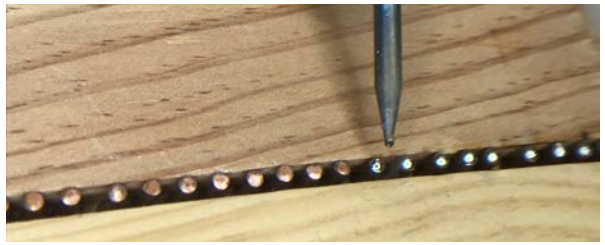
Bonus

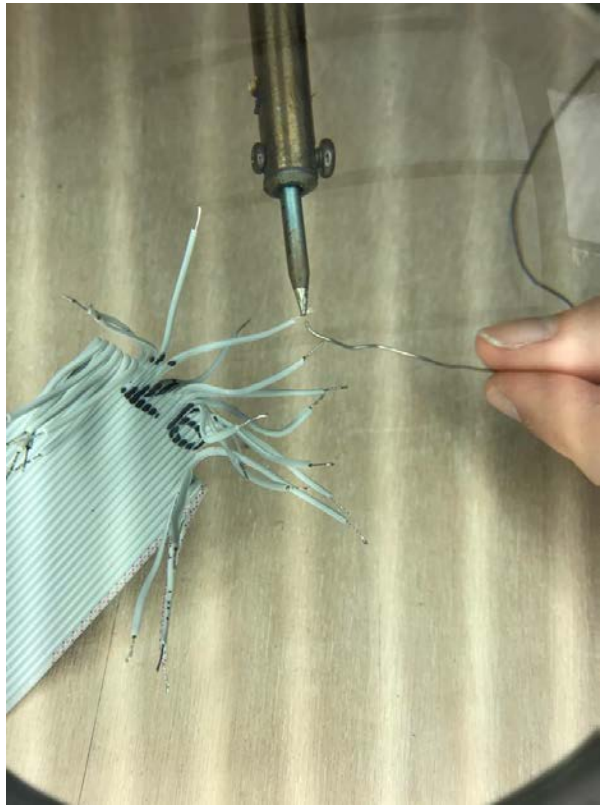
… soudures interminables d'une précision extrême (PCB et plus de 200 rivets dans les rotors)…





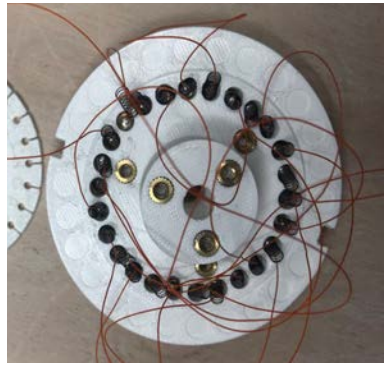


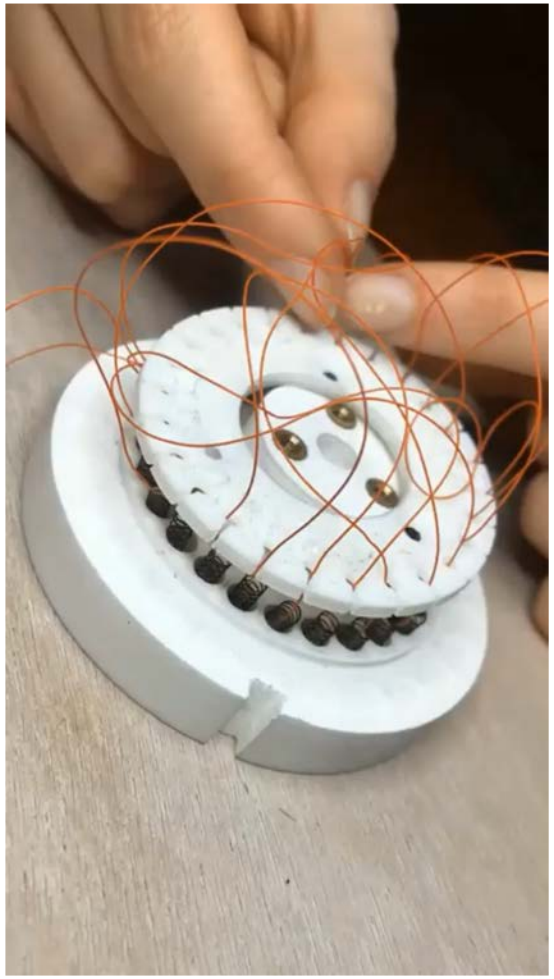


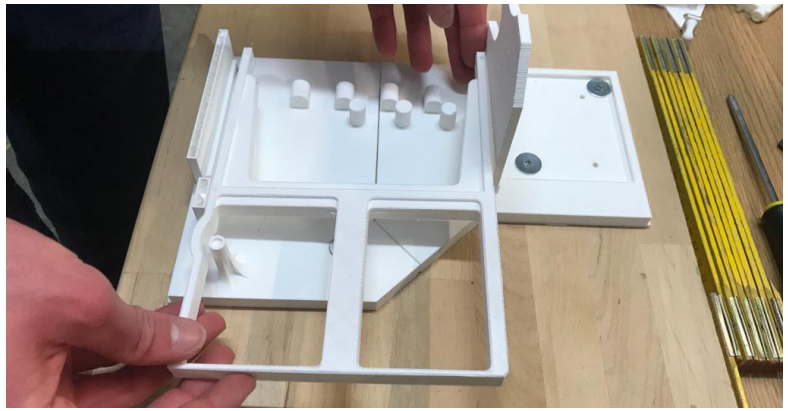


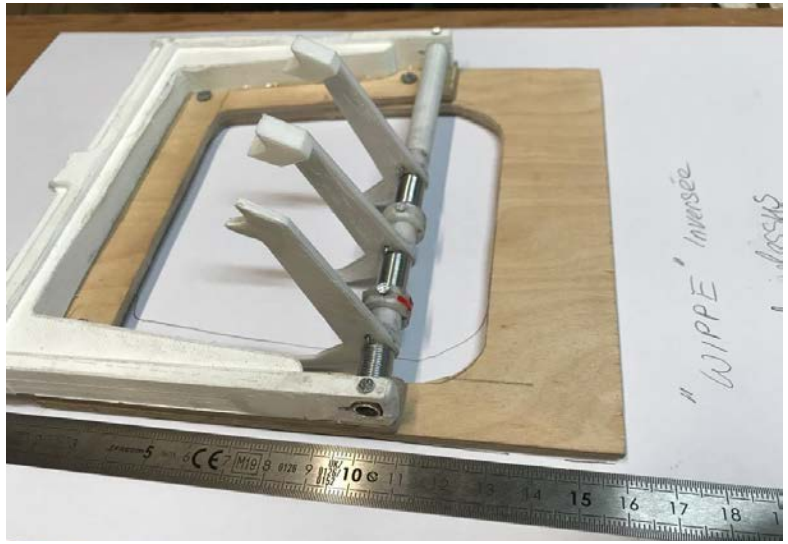
Bonus

… montage des rotors et de la structure…



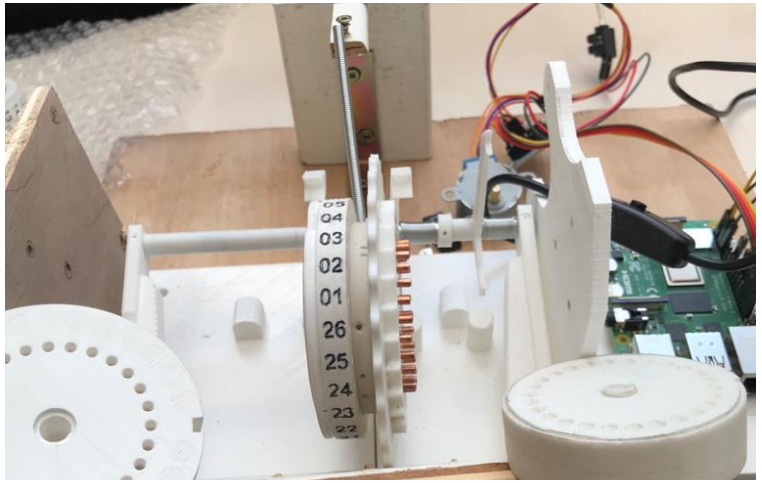


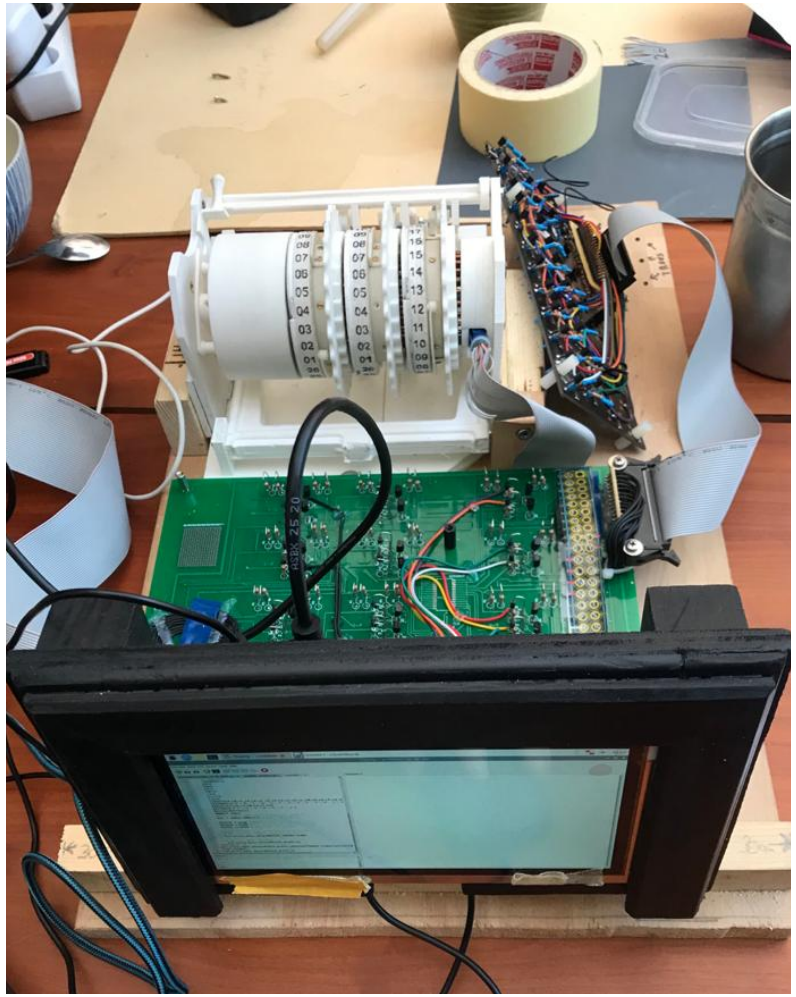


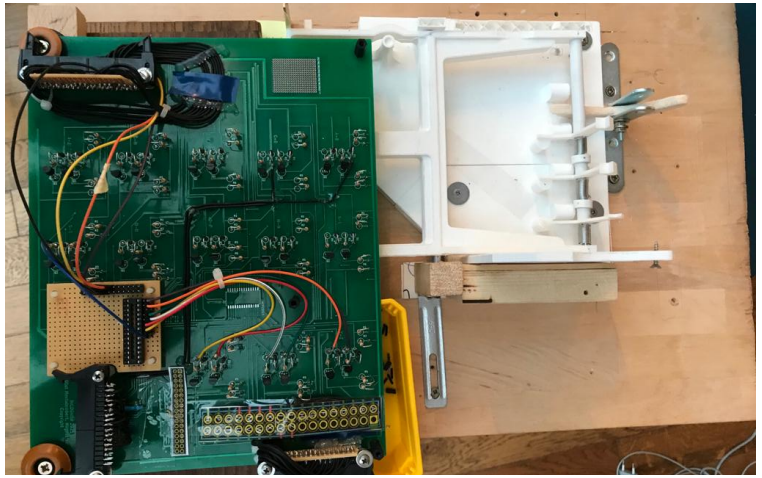


Bonus

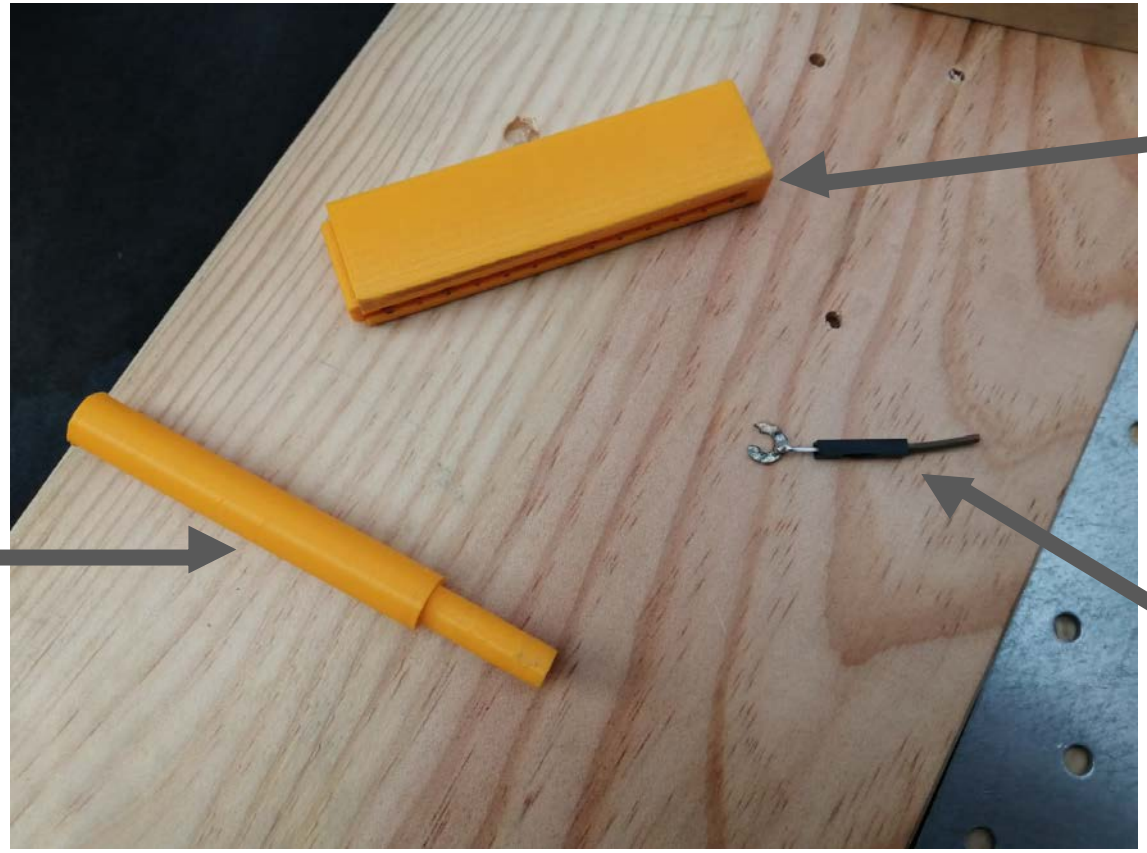
… enfin, la machine entière !!!







Un grand merci au Professeur Simon Wiest pour les outils et conseils fournis !!



Grinder
(poncer les têtes et queues des rivets)

Mounting pin
(monter les pièces de rotors)

Une de nos créations pour protéger le plastique des rotors pendant les soudures des rivets !

Que pourrions-nous améliorer ?

- **Informatique**
  - rendre le programme plus esthétique
  - Ajouter des fonctionnalités de chiffrement en temps réel
  - Modéliser le fonctionnement symétrique d'Enigma

- **Electronique**
  - Réduire la taille de la PCB (nous en étions à nos débuts sur le logiciel KiCAD)
  - Régler le problème de taille des broches femelles sur la PCB (trop petites)

- **Mécanique**
  - Utiliser une imprimante plus performante pour une meilleure qualité d'impression
  - Améliorer la sécurité des trajets du signal électrique à l'intérieur des rotors (soudures tombées, fils cassés, contacts trop enfoncés dans le plastique)
  - Réduire la taille globale de la machine InCOGnito et le temps de chiffrage
  - Accélérer le moteur
  - Construire une partie en bois à la place du plastique (pour améliorer la résistance)

Conclusion

Ce projet nous a accompagné durant les deux tiers de notre année de Terminale: c'est le premier projet autonome et extrascolaire où il a fallu investir autant de temps et d'énergie.

Il nous a permis de découvrir :

- l'importance de la rigueur dans la conception et la fabrication
- la nécessité d'une documentation complète
- les nuits presque blanches de recherches
- la joie et la fierté d'être responsable d'un projet complet

S'il nous a conforté dans notre volonté de travailler dans le domaine de l'ingénierie ou de l'innovation, nous avons surtout pu découvrir la fantastique atmosphère d'un groupe où chacun possède un rôle indispensable et différent.

Nous avons tous beaucoup appris à travers le projet InCOGnito, et ça CGENIAL !

Remerciements

Nous remercions le Professeur **Philippe Moiroud** pour son encadrement et plus généralement pour sa vision scientifique qui nous accompagne en qualité de professeur à l'institut Montalembert.
Nous remercions le rectorat de Créteil pour le financement de 100 €.
Nous remercions le concours Cgénial pour la bourse de 150 €.
Un grand merci à notre lycée **l'Institut Montalembert** pour la mise à disposition d'une imprimante 3D.

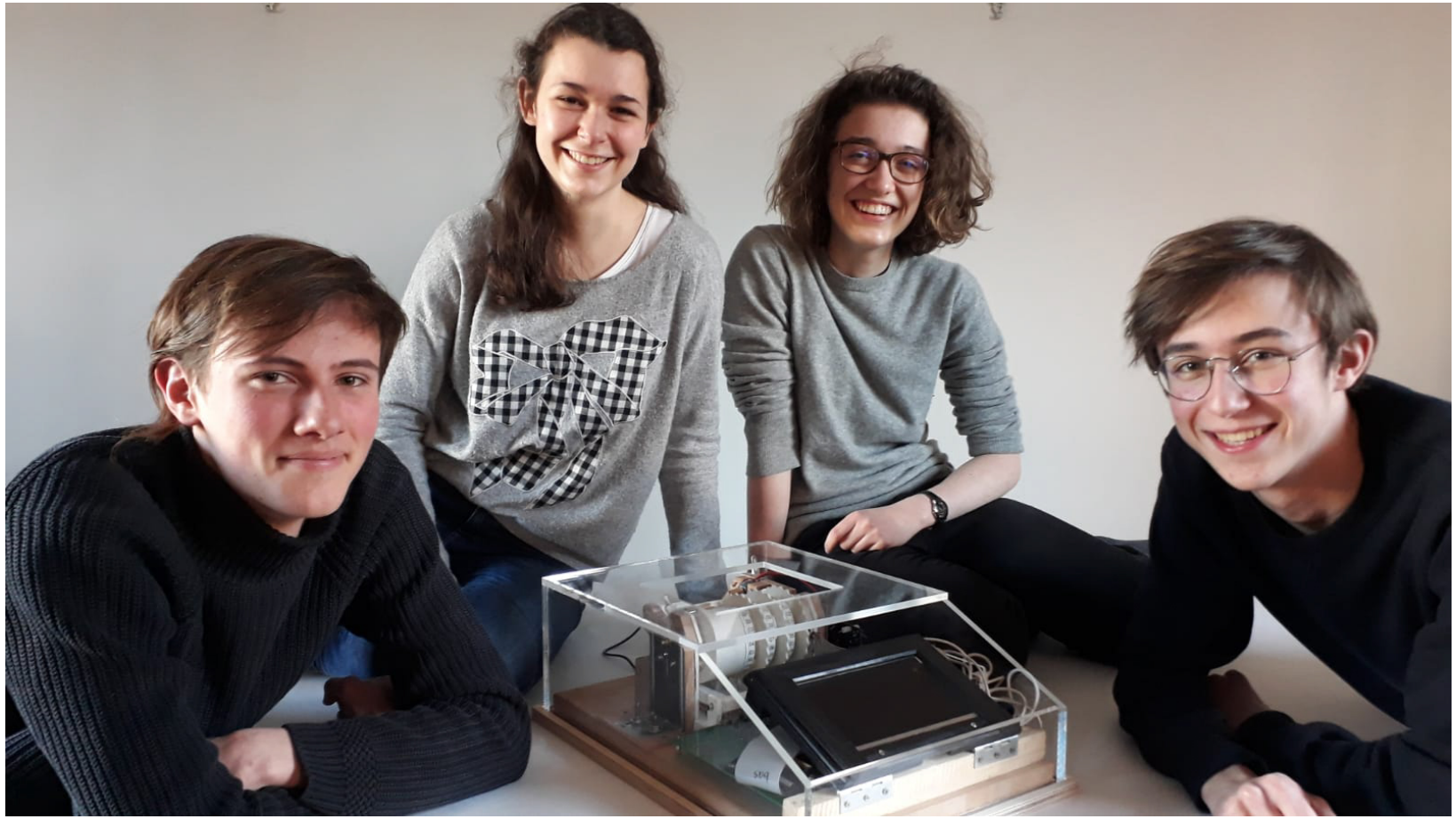
Nous souhaitons particulièrement remercier le Professeur **Simon Wiest** et l'école HDM de Stuttgart qui nous a alimenté avec des conseils et qui a mis à disposition les fichiers 3D nécessaires à la construction des rotors, bien en amont de la publication officielle du projet RDE (qui a duré 5 semestres).
Le projet Incognito s'inscrit dans la même logique de mettre à disposition ces résultats au grand public, et nos travaux seront accessibles pour toute personne voulant se baser sur notre travail (sur Internet).

Nous remercions Monsieur **Wolfgang Ertel,** de l'Institut de Weingarten qui a mis à disposition des plans de détails excellents de l'Enigma originale du projet Weingarten en 2011.

Nous remercions la **médiathèque Louis Aragon de Fontenay-sous-Bois** pour la mise à disposition de leur imprimante 3D afin de refaire des pièces à la dernière minute.

Nous remercions aussi nos parents pour leur soutien : **Sarah Bain**, ébéniste, pour la création de la boîte ; **Delphine Grenier**, artiste, pour son savoir-faire en résine et autres techniques plastiques qui nous ont aidés; nous remercions particulièrement **Adrian Meier**, ingénieur en électrotechnique, pour les conseils en gestion de projet ainsi qu'en fabrication mécanique et électrique.

Photo finale !



InCOGnito Team, mars 2021